Amendments to the Specification:

Please amend the paragraph beginning at page 2, line 1 as follows:

The IPSec session keys are typically established using Diffie-Hellman (DH) algorithm in the Internet Key Exchange (IFE) protocol. IKE also utilizes RSA and Digital Signature Algorithm (DSA) algorithns for Public Key Infra-structure (PKI). The algorithms used in SSL are RSA, DH, and DSA. RSA Is by far the most used algorithm in SSL protocol because its simplicity and its easy integration with PKI. However DH and DSA are also occasionally used in SSL. DSA is the algorithm favored by government agencies. Common to all three algorithms is the time-consuming modular exponentiation ($C = M^e \bmod N$) operation. One problem with the aforementioned security protocols is the time involved in computing the modular exponentiation ($C = M^e \bmod N$) operation. Typically, the values of C and N are both 1024 bits wide. The value of exponent e can also be as large as 1024 bits wide. [[The]] For example, the RSA private key decryption used by a server commonly has an exponent 1024 bits wide for stronger security. This means the calculation is extremely computation intensive, often resulting in relatively long delays before a secure connection is established. This problem is further compounded by the fact that the computation is typically performed by 32 or 64 bit microprocessor(s) in a server and not a dedicated device.